

# **[SECURITY PLAN TEMPLATE FOR THE PROTECTION OF CATEGORY 1 AND CATEGORY 2 QUANTITIES OF RADIOACTIVE MATERIAL AT COMMERCIAL POWER REACTOR FACILITIES]**

## **RADIOACTIVE MATERIALS SECURITY PLAN FOR [SITE/LICENSEE]**

### **1 INTRODUCTION**

The purpose of this Radioactive Materials Security Plan (Plan) is to provide a description of how the requirements of 10 CFR 37, “Physical Protection of Category 1 and Category 2 Quantities of radioactive Material” (Rule) are implemented at [Site(s)]. The intent of this Plan is to provide reasonable assurance of the security of category 1 or category 2 quantities of radioactive material by protecting these materials from theft or diversion as described in 10 CFR 37.41 – 57 (Subpart C – Physical Protection Requirements During Use). 10 CFR 37.43(a), “Security Plan,” requires a Security Plan to establish [Site/Licensee]’s overall security strategy to ensure the integrated and effective functioning of the security program required by Subpart C.

### **2 SECURITY PLAN**

#### **2.1 SCOPE AND PURPOSE**

10 CFR 37.43(a) requires each licensee identified in 10 CFR 37.41(a) to develop a written Security Plan (Plan) specific to its facilities and operations.

The purpose of this Plan is to establish [Site/Licensee]’s overall security strategy to ensure the integrated and effective functioning of the security program required by Subpart C.

The Plan describes the measures and strategies used to implement the requirements of Subpart C and identifies the security resources, equipment, and technology used to satisfy the requirements of Subpart C.

#### **2.2 PERFORMANCE REQUIREMENTS**

##### **PLAN APPROVAL, REVISION, AND RETENTION**

This Security Plan (Plan) shall be approved by the [Site/Licensee individual with overall responsibility for the security program].

This Plan shall be revised as necessary to ensure the effective implementation of Commission requirements. [Site/Licensee] shall ensure the revision has been reviewed and approved by the [Site/Licensee individual with overall responsibility for the security program]; and all affected [Site/Licensee] individuals are instructed on the revised Plan before the changes are implemented.

[Site/Licensee] shall retain a copy of this Plan as a record for 3 years after the Plan is no longer

required. If any portion of the Plan is superseded, [Site/Licensee] shall retain the superseded material for 3 years after the record is superseded.

## **IMPLEMENTING PROCEDURES**

[Site/Licensee] has developed and maintains written procedures that document how the requirements of Subpart C and this Plan will be met. These implementing procedures and revisions to these procedures are approved in writing by [the individual with overall responsibility for the security program]. [Site/Licensee] retains a copy of the current procedure as a record for 3 years after the procedure is no longer needed. Superseded portions of the procedure are retained for 3 years after the record is superseded.

[Site/Licensee] has elected to include implementing procedures as part of this document].

## **TRAINING**

[Site/Licensee] conducts training to ensure that those individuals implementing the security program possess and maintain the knowledge, skills, and abilities to carry out their assigned duties and responsibilities effectively.

The training includes instruction in the:

- Security program and procedures, and
- The purposes and functions of the security measures employed, and
- The responsibility to report promptly any condition that causes or may cause a violation of Commission requirements, and
- The responsibility of [Site/Licensee] to report promptly to the local law enforcement agency (LLEA) and [Site/Licensee] any actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material; and
- The appropriate response to security alarms.

In determining those individuals who shall be trained on the security program, [Site/Licensee] considers each individual's assigned activities during authorized use and response to potential situations involving actual or attempted theft, diversion, or sabotage of category 1 or category 2 quantities of radioactive material.

The extent of the training is commensurate with the individual's potential involvement in the security of category 1 or category 2 quantities of radioactive material.

Refresher training is provided at a frequency not to exceed 12 months and when significant changes have been made to the security program.

Refresher training includes:

- A review of the training requirements as stated above of and any changes made to the security program since the last training, and
- Reports on any relevant security issues, problems, and lessons learned, and

- Relevant results of NRC inspections, and
- Relevant results of the [Site/Licensee]'s program review and testing and maintenance.

[Site/Licensee] maintains records of the initial and refresher training for 3 years from the date of the training.

The training records include dates of the training, topics covered, a list of licensee personnel in attendance, and related information.

## PROTECTION OF INFORMATION

[Site/Licensee] limits access to and unauthorized disclosure of the Plan, implementing procedures, and the list of individuals that have been approved for unescorted access.

[Site/Licensee]'s efforts to limit access include the development, implementation, and maintenance of written policies and procedures for controlling access to, and for proper handling and protection against unauthorized disclosure of, the Plan and implementing procedures.

Before granting an individual access to the security plan or implementing procedures, [Site/Licensee] shall:

- Evaluate an individual's need to know the security plan or implementing Procedures, and
- If the individual has not been authorized for unescorted access to category 1 or category 2 quantities of radioactive material, safeguards information, or safeguards information modified handling, the [Site/Licensee] will complete a background investigation to determine the individual's trustworthiness and reliability.

A trustworthiness and reliability determination is conducted by a Reviewing Official and includes the background investigation elements contained in 10 CFR 37.25(a)(2) through (a)(7).

[Site/Licensee] need not subject the following individuals to the background investigation elements for protection of information:

- Individuals deemed trustworthy and reliable in accordance with the [Site/Licensee] Access Authorization program conducted in accordance with 10 CFR 73.56, or
- The categories of individuals listed in 10 CFR 37.29(a)(1) through (13), or
- Security service provider employees, provided written verification that the employee has been determined to be trustworthy and reliable, by the required background investigation defined within 10 CFR 37.25(a)(2) through (a)(7) or within 10 CFR 73.56 and this determination has been conveyed to [Site/Licensee] by the security service provider.

[Site/Licensee] documents the basis for concluding that an individual is trustworthy and reliable and should be granted access to the Plan or implementing procedures.

[Site/Licensee] maintains a list of persons currently approved for access to the Plan or implementing procedures.

When [Site/Licensee] determines that a person no longer needs access to the Plan or implementing procedures or no longer meets the access authorization requirements for access to the information, [Site/Licensee] removes the person from the approved list as soon as possible, but no later than 7 working days, and takes prompt measures to ensure that the individual is unable to obtain the Plan or implementing procedures.

When not in use, [Site/Licensee] stores its Plan and implementing procedures in a manner to prevent unauthorized access. Information stored in nonremovable electronic form is password protected.

[Site/Licensee] retains a copy of the information protection procedures and the list of individuals approved for access to the Plan or implementing procedures as a record for 3 years after the documents are no longer needed.

[Site/Licensee] protects any safeguards information or safeguards information modified handling in accordance with 10 CFR 73.21, 22, and 23 and all of the requirements of those sections.

#### **LOCAL LAW ENFORCEMENT AGENCY (LLEA) COORDINATION AND NOTIFICATION**

[Site/Licensee] coordinates, to the extent practicable, with an LLEA for responding to threats to [licensee's facility], including any necessary armed response. The information provided to the LLEA includes:

- A description of the facilities and the category 1 and category 2 quantities of radioactive materials along with a description of the [Site/Licensee] security measures that have been implemented to comply with this subpart, and
- Notification that [Site/Licensee] will request a timely armed response by the LLEA to any actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of material.

[Site/Licensee] notifies the appropriate NRC regional office within 3 business days if:

- The LLEA has not responded to the request for coordination within 60 days of the coordination request, or
- The LLEA notifies [the licensee] that the LLEA does not plan to participate in coordination activities.

[Site/Licensee] documents its efforts to coordinate with the LLEA. The documentation is kept for 3 years.

[Site/Licensee] coordinates with the LLEA at least every 12 months, or when changes to the facility design or operation adversely affect the potential vulnerability of [the licensee's] material to theft, sabotage, or diversion.

### **3 ESTABLISHING, IMPLEMENTING, AND MAINTAINING THE PHYSICAL ASPECTS OF THE RADIOACTIVE MATERIALS SECURITY PROGRAM**

This section establishes the requirements for the [Site/Licensee] physical protection program for aggregated category 1 or category 2 quantity of radioactive material listed in Appendix A of 10 CFR 37.

When implemented in accordance with the [Site/Licensee] procedures, these Plan attributes provide reasonable assurance of the security of category 1 or category 2 quantities of radioactive material by protecting these materials from theft or diversion.

#### **3.1 PHYSICAL CONTROLS ON ACCESS TO RADIOACTIVE MATERIALS**

[Category 1 and 2 quantities of radioactive material stored inside the PA are covered by requirements as delineated in the Physical Security Plan (PSP) for power reactors [describe any equipment that fits this criteria].]

[Category 1 and 2 quantities of radioactive material within the OCA are located such that they are covered by the requirements of 10 CFR Part 73.55(h)(5)(ii) which states, “Continuous surveillance, observation, and monitoring responsibilities may be performed by security personnel during continuous patrols through the use of video technology, or by a combination of both.”. Licensee security plans required by Part 73 implement that rule requirement. These materials are therefore exempt from the requirements of Part 37, in accordance with §37.11 [describe any equipment that fits this criteria].]

[Category 1 and 2 quantities of radioactive material associated with large equipment weighing in excess of 2000 kg (e.g., steam generators, reactor heads, contaminated turbine equipment, etc.) are considered self-protecting requiring specialized equipment and significant mission execution times to accomplish theft or diversion. Area monitoring (i.e. monitored intrusion detection system, monitored video surveillance system, routine work activities conducted by approved individuals, observation by approved individuals located within or outside the area, observation by approved individuals conducted in accordance with 10 CFR 73.55(h)(5)(ii)) in combination with the extensive mission execution aspects of this equipment satisfy the requirements of Part 37, in accordance with §37.11 [describe any equipment that fits this criteria and the determination basis (e.g. equipment location, equipment housing/shelter structure, monitoring methodology, monitoring frequency (if other than continuous))].]

#### **[SPECIFICALLY EXEMPTED MATERIALS AND THE DETERMINATION BASIS]**

[If category 1 and 2 quantities of radioactive material is located outside of protective measures provided by the Part 73 Security Plan, then additional measures shall be taken to ensure requirements of Part 37, Subpart C, are met as defined below.]

#### **[SECURITY ZONES EXTERNAL TO THE PROTECTED AREA NOT ADDRESSED BY PART 73]**

## SECURITY PLAN IMPLEMENTATION

[Site/Licensee] ensures that all aggregated category 1 and category 2 quantities of radioactive material are used or stored within [Site/Licensee] established security zones.

[Site/Licensee] Security zones may be permanent or temporary.

Temporary security zones are established as necessary to meet the [Site/Licensee]'s transitory or intermittent business activities, such as periods of maintenance, source delivery, and source replacement.

[Site/Licensee] Security zones, at a minimum, allow unescorted access only to approved individuals through:

- Isolation of category 1 and category 2 quantities of radioactive materials by the use of continuous physical barriers that allow access to the security zone only through established access control points. A physical barrier is a natural or man-made structure or formation sufficient for the isolation of the category 1 or category 2 quantities of radioactive material within a security zone, or
- Direct control of the security zone by approved individuals at all times, or a combination of continuous physical barriers and direct control.

For category 1 quantities of radioactive material during periods of maintenance, source receipt, preparation for shipment, installation, or source removal or exchange, [Site/Licensee] provides sufficient individuals approved for unescorted access to maintain continuous surveillance of sources in temporary security zones and in any security zone in which physical barriers or intrusion detection systems have been disabled to allow such activities.

Individuals not approved for unescorted access to category 1 or category 2 quantities of radioactive material are escorted by an [Site/Licensee] approved individual when in a security zone.

## MONITORING, DETECTION, AND ASSESSMENT

[Site/Licensee] establishes and maintains the capability to continuously monitor and detect without delay all unauthorized entries into security zones.

[Site/Licensee] provides the means to maintain continuous monitoring and detection capability in the event of a loss of the primary power source, or provide for an alarm and response in the event of a loss of this capability to continuously monitor and detect unauthorized entries.

Monitoring and detection is performed by:

- A monitored intrusion detection system that is linked to an onsite or offsite central monitoring facility, or
- Electronic devices for intrusion detection alarms that will alert nearby [Site/Licensee] personnel, or
- A monitored video surveillance system, or

- Direct visual surveillance by [Site/Licensee] approved individuals located within the security zone, or
- Direct visual surveillance by a [Site/Licensee] designated individual located outside the security zone.

[Site/Licensee] has a means to detect unauthorized removal of the radioactive material from the security zone.

This detection capability provides:

- For category 1 quantities of radioactive material, immediate detection of any attempted unauthorized removal of the radioactive material from the security zone.  
Immediate detection capability is provided by:
  - Electronic sensors linked to an alarm, or
  - Continuous monitored video surveillance; or
  - Direct visual surveillance.
- For category 2 quantities of radioactive material, weekly verification through physical checks, tamper indicating devices, use, or other means to ensure that the radioactive material is present.

[Site/Licensee] immediately assesses each actual or attempted unauthorized entry into the security zone to determine whether the unauthorized access was an actual or attempted theft, sabotage, or diversion.

Personnel and automated or electronic systems supporting the [Site/Licensee]'s monitoring, detection, and assessment systems:

- Maintain continuous capability for personnel communication and electronic data transmission and processing among [Site/Licensee] site security systems, and
- Provide an alternative communication capability for personnel, and an alternative data transmission and processing capability, in the event of a loss of the primary means of communication or data transmission and processing.

Alternative communications and data transmission systems may not be subject to the same failure modes as the primary systems.

[Site/Licensee] immediately initiates a response to any actual or attempted unauthorized access to the security zones, or actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material at licensee facilities or temporary job sites by requesting, without delay, an armed response from the LLEA.

## **MAINTENANCE AND TESTING**

[Site/Licensee] implements a maintenance and testing program to ensure that intrusion alarms, associated communication systems, and other physical components of the systems used to secure or detect unauthorized access to radioactive material are maintained in operable condition and are capable of performing their intended function when needed.

The equipment relied on to meet the [Site/Licensee] radioactive materials security requirements is inspected and tested for operability and performance at the manufacturer's suggested frequency.

If there is no suggested manufacturer's suggested frequency, the testing is performed at least annually, not to exceed 12 months.

[Site/Licensee] maintains records on the maintenance and testing activities for 3 years.

## **MOBILE DEVICE CONTROL**

Any mobile devices containing category 1 or category 2 quantities of radioactive material:

- Has two independent physical controls that form tangible barriers to secure the material from unauthorized removal when the device is not under direct control and constant surveillance by [Site/Licensee] approved individuals, and
- For devices in or on a vehicle or trailer, unless the health and safety requirements prohibit the disabling of the vehicle, [Site/Licensee] utilizes a method to disable the vehicle or trailer when not under direct control and constant surveillance [Site/Licensee] approved individuals. [Site/Licensee] does not rely on the removal of an ignition key to meet this requirement.

## **SECURITY PROGRAM REVIEW**

[Site/Licensee] is responsible for the continuing effectiveness of the security program.

[Site/Licensee] ensures that the security program is reviewed to confirm compliance with the requirements of Subpart C and that comprehensive actions are taken to correct any noncompliance that is identified. The review must include the radioactive material security program content and implementation.

[Site/Licensee] periodically (at least annually) reviews the security program content and implementation.

The results of the review, along with any recommendations, are documented. Each review report must identify conditions that are adverse to the proper performance of the security program, the cause of the condition(s), and, when appropriate, recommends corrective actions, and corrective actions taken. [Site/Licensee] reviews the findings and takes any additional corrective actions necessary to preclude repetition of the condition, including reassessment of the deficient areas where indicated.

[Site/Licensee] maintains the review documentation for 3 years.

## **EVENT REPORTING**

[Site/Licensee] immediately notifies the LLEA after determining that an unauthorized entry

resulted in an actual or attempted theft, sabotage, or diversion of a category 1 or category 2 quantity of radioactive material.

As soon as possible after initiating the response, but not at the expense of causing delay or interfering with the LLEA response to the event, [Site/Licensee] notifies the NRC's Operations Center (301-816- 5100).

In no case shall the notification to the NRC be later than 4 hours after the discovery of any attempted or actual theft, sabotage, or diversion.

[Site/Licensee] shall assess any suspicious activity related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material and notify the LLEA as appropriate.

As soon as possible but not later than 4 hours after notifying the LLEA, [the licensee] shall notify the NRC's Operations Center (301-816- 5100).

The initial telephonic notification shall be followed within a period of 30 days by a written report submitted to the NRC by an appropriate method listed in 10 CFR 37.7. The report must include sufficient information for NRC analysis and evaluation, including identification of any necessary corrective actions to prevent future instances.

[THIS PAGE IS LEFT BLANK INTENTIONALLY]